



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,882	07/08/2003	Philip Michael Hawkes	030441	9835
23696	7590	07/08/2009		
QUALCOMM INCORPORATED 5775 MOREHOUSE DR. SAN DIEGO, CA 92121			EXAMINER SIMITOSKI, MICHAEL J	
			ART UNIT 2439	PAPER NUMBER
			NOTIFICATION DATE 07/08/2009	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com

kascanla@qualcomm.com

nanm@qualcomm.com

Office Action Summary

Application No.

10/615,882

Applicant(s)

HAWKES ET AL.

Examiner

MICHAEL J. SIMITOSKI

Art Unit

2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 April 2009.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 64-86 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 64-86 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 19 September 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/5508)
Paper No(s)/Mail Date _____

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____

DETAILED ACTION

1. The response of 4/30/2009 was received and considered.
2. Claims 64-86 are pending.

Response to Arguments

3. Applicant's arguments filed 4/30/2009 have been fully considered but they are not persuasive.
 - a. Applicant's attention is directed to the responses in the Advisory Action of 2/2/09 to Applicant's after-final arguments.
 - b. Applicant's response (p. 9, ¶3) argues that the KEK in Ahonen is a subscriber-specific key, in contrast to Hawkes's BAK, which is not and therefore, the idea that the KEK in Ahonen is encrypted with a public key is not applicable to Hawkes. However, it is submitted that the teaching of simple key distribution is sufficient to draw a parallel between Hawkes and Ahonen. Briefly, "simple" is used because whereas Hawkes's invention must initially determine a way to share a key between to devices for encryption of another key, in Ahonen's public-key encryption scheme it does not matter how the initial keys are shared and the provider of Ahonen does not need to store the public keys securely, as no subscriber can use another subscriber's public key to decrypt a message encrypted with the public key known to the provider. Referring to "drawing a parallel", each of Hawkes and Ahonen initially use a "top" encryption key to encrypt a "lower" encryption key. Hawkes uses symmetric key (same key at both ends), whereas Ahonen uses public key (sending end has a public key, receiving end has a private key), where a message encrypted with the public key can only be decrypted by the corresponding private key. As described above, there are clear benefits to public key encryption over symmetric key and these benefits were known to a skilled artisan at the time the invention was made. Therefore, the rejection is maintained.

c. Applicant's response (p. 9, ¶4 - p. 10, ¶1) argues that Hawkes's discussion of public key cryptography somehow reduces or destroys the known benefits of public key cryptography as it would apply to Hawkes's invention. However, the cited portion of Hawkes clearly states that (and only that) some other mechanism is required to provide authentication. However, Hawkes does not teach away from using public key cryptography for encryption and decryption. Further, it is well known in any art that technology generally has advantages and disadvantages and one having ordinary skill in the art at the time of the invention would not have construed the existence of a disadvantage of public key cryptography to rule out its use entirely, as suggested by Applicant.

d. Applicant's response (p. 10, ¶1) further argues that Ahonen "expresses similar concerns". However, once again, the cited portion of Ahonen clearly states that (and only that) PKI uses certificates for authentication. However, Ahonen does not teach away from using public key cryptography for encryption and decryption. Further (and again as stated above), it is well known in any art that technology generally has advantages and disadvantages and one having ordinary skill in the art at the time of the invention would not have construed the existence of a disadvantage of public key cryptography to rule out its use entirely, as suggested by Applicant. In this case, the usage of a public key generally suggests a determination of its validity. However, it is believed that a skilled artisan at the time of the invention would have been able to weigh the determination of validity against the ease of distribution and usage to find the use of PKI instead of symmetric key cryptography an obvious modification.

e. Applicant's response (p. 10, ¶2) suggests that the Examiner has provided no factual basis for the rejection. However, it is noted that Applicant's own submission of prior art (11/30/2004, regarding the Menezes reference, p. 551) discusses advantages offered by public-key (vs. symmetric-key) techniques. The question under consideration in this case is whether a skilled

Art Unit: 2439

artisan would have found it *obvious* to modify Hawkes to use public-key techniques in the top level key, rather than symmetric-key techniques. Based on the Ahonen reference actually using the technique and the Menezes reference (dated 1997) and further on the general ubiquity of both public-key and symmetric-key usage, the Examiner maintains that such a skilled artisan would have found it obvious to interchange the two and that such a modification would have required no undue experimentation and would not destroy the Hawkes reference.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 64-69, 71-75, 77-80 & 82-85 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication 2002/0141591, published 11/3/2002 to Hawkes et al. (**Hawkes**) in view of U.S. Patent Application Publication 2006/0168446 to Ahonen et al. (**Ahonen**).

Regarding claim 64, Hawkes discloses a method for broadcasting encrypted multimedia content from a content provider (content server, ¶63) to a plurality of authorized terminals (MS) over the air (¶57), comprising each terminal having a mobile equipment (ME, Fig. 4, #306) and having a secure processing unit (UIM, Fig. 4, #308) that securely stores a unique key (RK is stored in SUMU, Fig. 4, #314, ¶74) that is not accessible to a terminal user (SUMU discourages unauthorized access to the information, ¶65), and wherein the content provider (CS) encrypts a broadcast access key (BAK) with each of the unique keys (RK) to authorize a terminal having the secure processing unit securely storing a corresponding key to receive the encrypted multimedia content (BAK is encrypted with RK, ¶74), each terminal receiving the respective encrypted broadcast access key (BAK) over the air from the content

Art Unit: 2439

provider (BAK1 is received from CS, ¶74) and providing the respective encrypted broadcast access key (BAK1 is passed to the UIM, ¶74) to the terminal's secure processing unit (UIM, ¶74), wherein the terminal's secure processing unit (UIM) decrypts the encrypted broadcast access key (BAK1) using the secure processing unit's unique key (RK is used in the UIM to decrypt BAK from BAK1, ¶74) and securely stores the broadcast access key (BAK is stored in SUMU, ¶74), each terminal receiving short-term key information (SKI, ¶76 & ¶78) and encrypted multimedia content (received broadcast content, ¶80) over the air from the content provider (CS) to the terminals (MS, ¶76 & ¶80), wherein the content is encrypted with a short-term key (¶81), and wherein the short-term key is generated using the broadcast access key (BAK) and short-term key information (SKI and BAK are processed to determine SK, ¶76), and provides the short-term key (SK) to the terminal's mobile equipment (SK is passed to ME, ¶80-81, last two lines of each), and each terminal's mobile equipment decrypting the multimedia content using the short-term key (ME decrypts the received broadcast content, ¶80-81, last two lines of each). Hawkes lacks each terminals forwarding a unique public key over the air to the content provider and lacks wherein the secure processing unit stores a unique private key (instead of Hawkes's RK), corresponding to the unique public key. However, Ahonen teaches a system where a terminal forwards a unique public key over the air (over a 3G network, ¶37) to a content provider (terminal sends a registration message to a group controller, the message including a copy of the terminal's public key, ¶38), wherein each terminal stores a unique private key corresponding to the unique public key (terminal creates a signature using the private key, ¶38 & ¶42, showing that the terminal stores the private key). Similarly to Hawkes's RK, the private key that corresponds to the forwarded unique public key in Ahonen is used to decrypt a received encrypted key encrypting key (KEK), which is similar to Hawkes's BAK (¶41). The KEK is then used to decrypt a received encrypted traffic encrypting key (TEK, ¶41) which decrypts the broadcast content (¶36) that is received, possibly from the group controller (¶19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hawkes such that each

Art Unit: 2439

terminal (MS) forwards a unique public key over the air to the content provider (CS), wherein the secure processing unit (UIM) stores a unique private key (instead of Hawkes's RK), corresponding to the unique public key. One of ordinary skill would have been motivated to perform this modification to achieve a simple mechanism for key dissemination, as taught by Ahonen (¶7). One of ordinary skill in the art at the time the invention was made would appreciate this benefit because Ahonen is using the existing, well-known, public key infrastructure to share a key, rather than a more complex protocol such as AKA or IKE.

Regarding claim 65, Hawkes, as modified above, discloses wherein the short-term key (SK) is accessible to a user (Hawkes discloses that data in the ME is easily accessed, ¶64 and that SK is passed to the ME for decrypting of the broadcast content, ¶78; therefore, the SK is accessible to a user).

Regarding claim 66, Hawkes, as modified above, discloses wherein the short-term key is changed by the content provider at a rate such that the cost of an unauthorized terminal user obtaining the short-term key from the mobile equipment exceeds the value of the short-term key to the unauthorized terminal user (Hawkes discloses that the SK is changed frequently such that the cost of a non-subscriber obtaining SK from the memory exceeds the value of SK, ¶68).

Regarding claim 67, Hawkes, as modified above, discloses wherein the secure processing unit (UIM) is removable from the terminal (¶66).

Regarding claim 68, Hawkes, as modified above, discloses wherein the short-term key information (SKI) is the short-term key encrypted using the broadcast access key (SKI may be the encryption of SK using BSK as the key, ¶76).

Regarding claim 69, Hawkes, as modified above, discloses wherein the short-term key (SK) is generated by applying a cryptographic hash to a concatenation of the short-term key information (SKI) and the broadcast access key (BAK, ¶76, last three lines).

Regarding claim 71, Hawkes, as modified above, discloses wherein at least one terminal (MS) comprises a mobile station (Fig. 3, #206 & ¶57).

Regarding claim 72, Hawkes discloses an integrated circuit (¶107) for a mobile station (MS, Fig. 4, #300) comprising means for securely storing a unique key (RK is stored in SUMU, Fig. 4, #314, ¶74) that is not accessible to a terminal user (SUMU discourages unauthorized access to the information, ¶65), and wherein the content provider (CS) encrypts a broadcast access key (BAK) with each of the unique keys (RK) to authorized an integrated circuit securely storing a corresponding key to receive the encrypted multimedia content (BAK is encrypted with RK, ¶74 and RK is stored in the UIM, ¶74), means (MS) for receiving the respective encrypted broadcast access key (BAK) over the air from the content provider (BAK is received from CS, ¶74), means (MS) for decrypting the encrypted broadcast access key (BAK) using the secure processing unit's unique key (RK is used in the UIM to decrypt BAK from BAKI, ¶74) and securely storing the broadcast access key (BAK is stored in SUMU, ¶74), wherein the securely stored broadcast access key is not accessible to a user (SUMU discourages unauthorized access to the information, ¶65 and the BAK is stored in the SUMU, ¶74), means (MS) for receiving short-term key information (SKI, ¶76 & ¶78) and encrypted multimedia content (received broadcast content, ¶80) over the air from the content provider (CS) to the a plurality of mobile stations (Fig. 3, #206) each having the integrated circuit (MS, ¶76 & ¶80, Fig. 4, #300), wherein the content is encrypted with a short-term key (¶81), and wherein the short-term key is generated using the broadcast access key (BAK) and short-term key information (SKI and BAK are processed to determine SK, ¶76), means (MS) for generating the short term key using the securely stored broadcast access key (BAK) and the broadcast short-term key information (SKI and BAK are processed to determine SK, ¶76) and means (MS) for decrypting the multimedia content using the short-term key (ME decrypts the received broadcast content using SK, ¶¶80-81, last two lines of each). Hawkes lacks forwarding a unique public key over the air to the content provider and lacks securely storing a unique private key (instead of Hawkes's RK), corresponding to the

Art Unit: 2439

unique public key. However, Ahonen teaches a system where a terminal forwards a unique public key over the air (over a 3G network, ¶37) to a content provider (terminal sends a registration message to a group controller, the message including a copy of the terminal's public key, ¶38), wherein each terminal stores a unique private key corresponding to the unique public key (terminal creates a signature using the private key, ¶38 & ¶42, showing that the terminal stores the private key). Similarly to Hawkes's RK, the private key that corresponds to the forwarded unique public key in Ahonen is used to decrypt a received encrypted key encrypting key (KEK), which is similar to Hawkes's BAK (¶41). The KEK is then used to decrypt a received encrypted traffic encrypting key (TEK, ¶41) which decrypts the broadcast content (¶36) that is received, possibly from the group controller (¶19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hawkes's terminal such that each terminal (MS) forwards a unique public key over the air to the content provider (CS), wherein the secure processing unit (UIM) stores a unique private key (instead of Hawkes's RK), corresponding to the unique public key. One of ordinary skill would have been motivated to perform this modification to achieve a simple mechanism for key dissemination, as taught by Ahonen (¶7). One of ordinary skill in the art at the time the invention was made would appreciate this benefit because Ahonen is using the existing, well-known, public key infrastructure to share a key, rather than a more complex protocol such as AKA or IKE.

Regarding claim 73, Hawkes, as modified above, discloses wherein the short-term key (SK) is accessible to a user (Hawkes discloses that data in the ME is easily accessed, ¶64 and that SK is passed to the ME for decrypting of the broadcast content, ¶78; therefore, the SK is accessible to a user).

Regarding claim 74, Hawkes, as modified above, discloses wherein the short-term key information (SKI) is the short-term key encrypted using the broadcast access key (SKI may be the encryption of SK using BSK as the key, ¶76).

Regarding claim 75, Hawkes, as modified above, discloses wherein the short-term key (SK) is generated by applying a cryptographic hash to a concatenation of the short-term key information (SKI) and the broadcast access key (BAK, ¶76, last three lines).

Regarding claim 77, Hawkes discloses a machine-readable medium (¶108) comprising code for securely storing a unique key (RK is stored in SUMU, Fig. 4, #314, ¶74) that is not accessible to a terminal user (SUMU discourages unauthorized access to the information, ¶65), and wherein the content provider (CS) encrypts a broadcast access key (BAK) with each of the unique keys (RK) to authorized a terminal securely storing a corresponding key to receive the encrypted multimedia content (BAK is encrypted with RK, ¶74 and RK is stored in the UIM, ¶74), code (MS, ¶108) for receiving the respective encrypted broadcast access key (BAK) over the air from the content provider (BAK is received from CS, ¶74), code (MS, ¶108) for decrypting the encrypted broadcast access key (BAK) using the secure processing unit's unique key (RK is used in the UIM to decrypt BAK from BAKI, ¶74) and securely storing the broadcast access key (BAK is stored in SUMU, ¶74), wherein the securely stored broadcast access key is not accessible to a user (SUMU discourages unauthorized access to the information, ¶65 and the BAK is stored in the SUMU, ¶74), code (MS, ¶108) for receiving short-term key information (SKI, ¶76 & ¶78) and encrypted multimedia content (received broadcast content, ¶80) over the air from the content provider (CS) to the a plurality of terminals (Fig. 3, #206) each having a integrated circuit (MS, ¶76, ¶80 & ¶107, Fig. 4, #300), wherein the multimedia content is encrypted with a short-term key (¶81), and wherein the short-term key is generated using the broadcast access key (BAK) and short-term key information (SKI and BAK are processed to determine SK, ¶76), code (MS, ¶108) for generating the short term key using the securely stored broadcast access key (BAK) and the broadcast short-term key information (SKI and BAK are processed to determine SK, ¶76) and code (MS, ¶108) for decrypting the multimedia content using the short-term key (ME decrypts the received broadcast content using SK, ¶¶80-81, last two lines of each). Hawkes lacks forwarding a unique public key over the air to the content

Art Unit: 2439

provider and lacks securely storing a unique private key (instead of Hawkes's RK), corresponding to the unique public key. However, Ahonen teaches a system where a terminal forwards a unique public key over the air (over a 3G network, ¶37) to a content provider (terminal sends a registration message to a group controller, the message including a copy of the terminal's public key, ¶38), wherein each terminal stores a unique private key corresponding to the unique public key (terminal creates a signature using the private key, ¶38 & ¶42, showing that the terminal stores the private key). Similarly to Hawkes's RK, the private key that corresponds to the forwarded unique public key in Ahonen is used to decrypt a received encrypted key encrypting key (KEK), which is similar to Hawkes's BAK (¶41). The KEK is then used to decrypt a received encrypted traffic encrypting key (TEK, ¶41) which decrypts the broadcast content (¶36) that is received, possibly from the group controller (¶19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hawkes's terminal such that each terminal (MS) comprises code that forwards a unique public key over the air to the content provider (CS), wherein the terminal includes code for storing securely a unique private key (instead of Hawkes's RK), corresponding to the unique public key. One of ordinary skill would have been motivated to perform this modification to achieve a simple mechanism for key dissemination, as taught by Ahonen (¶7). One of ordinary skill in the art at the time the invention was made would appreciate this benefit because Ahonen is using the existing, well-known, public key infrastructure to share a key, rather than a more complex protocol such as AKA or IKE.

Regarding claim 78, Hawkes, as modified above, discloses wherein the short-term key (SK) is accessible to a user (Hawkes discloses that data in the ME is easily accessed, ¶64 and that SK is passed to the ME for decrypting of the broadcast content, ¶78; therefore, the SK is accessible to a user).

Regarding claim 79, Hawkes, as modified above, discloses wherein the short-term key information (SKI) is the short-term key encrypted using the broadcast access key (SKI may be the encryption of SK using BSK as the key, ¶76).

Art Unit: 2439

Regarding claim 80, Hawkes, as modified above, discloses wherein the short-term key (SK) is generated by applying a cryptographic hash to a concatenation of the short-term key information (SKI) and the broadcast access key (BAK, ¶76, last three lines).

Regarding claim 82, Hawkes discloses an apparatus (MS, Fig. 4, #300) for receiving encrypting multimedia content broadcast over the air (Fig. 3, #206) from a content provider (CS, ¶63) to a plurality of authorized apparatuses (Fig. 3, #206) comprising a mobile equipment (ME, Fig. 4, #306) configured to decrypt the multimedia content using the short-term key (ME decrypts the received broadcast content using SK, ¶¶80-81, last two lines of each), wherein the multimedia content is encrypted with the short-term key (SK, ¶81), and wherein the short-term key is generated using the broadcast access key (BAK) and short-term key information (SKI and BAK are processed to determine SK, ¶76), and a secure processing unit (UIM, Fig. 4, #308) configured to securely store a unique key (RK is stored in SUMU, Fig. 4, #314, ¶74) that is not accessible to a terminal user (SUMU discourages unauthorized access to the information, ¶65), and wherein the content provider (CS) encrypts a broadcast access key (BAK) with the unique key (RK) to authorize an apparatus having the secure processing unit (authorize the MS) securely storing the corresponding key (RK) to receive the encrypted multimedia content (BAK is encrypted with RK, ¶74 and RK is stored in the UIM, ¶74), receive the respective encrypted broadcast access key (BAK) over the air (Fig. 3, #206) from the content provider (BAKI is received from CS, ¶74), decrypt the encrypted broadcast access key (BAKI; RK is used in the UIM to decrypt BAK from BAKI, ¶74) and securely store the broadcast access key (BAK is stored in SUMU, ¶74), wherein the securely stored broadcast access key is not accessible to a user (SUMU discourages unauthorized access to the information, ¶65 and the BAK is stored in the SUMU, ¶74), receive the short-term key information (SKI) broadcast over the air from the content provider (CS sends SKI to MS, ¶76) and generating the short-term key using the securely stored broadcast access key (BAK) and broadcast short-term key information (SKI and BAK are processed to determine SK, ¶76). Hawkes lacks the mobile equipment forwarding a unique

Art Unit: 2439

public key over the air to the content provider and lacks the secure processing unit securely storing a unique private key (instead of Hawkes's RK), corresponding to the unique public key. However, Ahonen teaches a system where a terminal forwards a unique public key over the air (over a 3G network, ¶37) to a content provider (terminal sends a registration message to a group controller, the message including a copy of the terminal's public key, ¶38), wherein each terminal stores a unique private key corresponding to the unique public key (terminal creates a signature using the private key, ¶38 & ¶42, showing that the terminal stores the private key). Similarly to Hawkes's RK, the private key that corresponds to the forwarded unique public key in Ahonen is used to decrypt a received encrypted key encrypting key (KEK), which is similar to Hawkes's BAK (¶41). The KEK is then used to decrypt a received encrypted traffic encrypting key (TEK, ¶41) which decrypts the broadcast content (¶36) that is received, possibly from the group controller (¶19). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hawkes's terminal such that the mobile equipment (ME) forwards a unique public key over the air to the content provider (CS) and the secure processing unit (UIM) stores a unique private key (instead of Hawkes's RK), corresponding to the unique public key. One of ordinary skill would have been motivated to perform this modification to achieve a simple mechanism for key dissemination, as taught by Ahonen (¶7). One of ordinary skill in the art at the time the invention was made would appreciate this benefit because Ahonen is using the existing, well-known, public key infrastructure to share a key, rather than a more complex protocol such as AKA or IKE.

Regarding claim 83, Hawkes, as modified above, discloses wherein the short-term key (SK) is accessible to a user (Hawkes discloses that data in the ME is easily accessed, ¶64 and that SK is passed to the ME for decrypting of the broadcast content, ¶78; therefore, the SK is accessible to a user).

Regarding claim 84, Hawkes, as modified above, discloses wherein the short-term key information (SKI) is the short-term key encrypted using the broadcast access key (SKI may be the encryption of SK using BSK as the key, ¶76).

Regarding claim 85, Hawkes, as modified above, discloses wherein the short-term key (SK) is generated by applying a cryptographic hash to a concatenation of the short-term key information (SKI) and the broadcast access key (BAK, ¶76, last three lines).

6. Claims 70, 76, 81 & 86 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hawkes and Ahonen**, as applied to claims 69, 75, 80 & 85 above, in further view of Applied Cryptography, Second Edition by Bruce Schneier (**Schneier**).

Regarding claims 70, 76, 81 & 86, Hawkes, as modified above, discloses wherein the short-term information is at least partly unpredictable, but lacks explicitly where it is a random value. However, Schneier discloses that good keys for encryption are random, such that all possible values are equally likely (i.e. unpredictable, p. 173, §Random Keys, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hawkes invention, as modified above, such that the short-term information is a random value. One of ordinary skill in the art would have been motivated to perform such a modification to enhance the security of the encrypted data such that the key is unpredictable via its randomness, as taught by Schneier.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2439

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

July 1, 2009

/Michael J Simitoski/

Primary Examiner, Art Unit 2439